

AD-A198 346

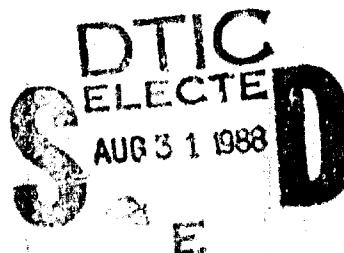
Report No. 38009

ROYAL SIGNALS AND RADAR ESTABLISHMENT,
MALVERN

ON THE PRIVACY PROBLEMS
INVOLVED IN ALLOWING ACCESS
TO COMPUTERS VIA THE
PUBLIC TELEPHONE SYSTEM

Author: Dr S C Glass

BEST
AVAILABLE COPY



PROCUREMENT EXECUTIVE, MINISTRY OF DEFENCE
RSRE

Malvern, Worcestershire.

April 1988

UNLIMITED

ROYAL SIGNALS AND RADAR ESTABLISHMENT

Report 88006

Title: ON THE PRIVACY PROBLEMS INVOLVED IN ALLOWING ACCESS
TO COMPUTERS VIA THE PUBLIC TELEPHONE SYSTEM

Author: S C Giess

Date: April 1988

SUMMARY

This report discusses some privacy problems involved in allowing access to computers over the Public Switched Telephone Network (PSTN).

The relevant aspects of current land-line PSTN and cellular radio operations are described and the weaknesses of the access controls of current computer systems are discussed. Possible solutions that would allow access under a limited set of conditions are described.

Copyright
C
Controller HMSO London
1988

i

0114 1988-1
COPY 4

Accession For	
NTIS GRAB	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

Contents

- 1 Introduction
- 2 Public Switched Telephone Network
- 3 Evesdropping and radio links in the communications chain
- 4 Modems and their operation
- 5 Current methods of access control
- 6 Possible courses of action
- 7 Are all the techniques always applicable?
- 8 Conclusions

Reference

1 Introduction

The increasing use of computers for data transfer and manipulation has lead to a desire for greater access to the services provided on central computers from remote points. A big stimulus has come from the widespread use of personal computers for word processing, electronic mail and the interactive database systems such as Prestel. Communications between the central systems and personal computers are usually carried out by means of interface devices called modems. These are attached to the computers at both ends and use the Public Switched Telephone Network (PSTN) to convey the data.

This use of the PSTN for remote access is flexible but it can entail certain risks. In particular, ANYBODY who knows the telephone number of a computer service can attempt to access it using a modem even if unauthorised to do so. This has lead to the rise of the "hacker" phenomenon; people trying to access computers they should not, usually treating the matter more as a challenge than anything else. These people would merely be a nuisance if that was all that they tried to do. However there are some whose actions, whether by design or by accident, seriously compromise both computer systems and the data held on them.

Commercial and University organisations often acquiesce, albeit reluctantly, to this state of affairs. Clearly the special role of Government and its institutions imposes a greater need to protect the integrity of its computer-based data systems. One way to achieve this protection would be to forbid the accessing of Government data over PSTN connections. Such an approach may be over restrictive as ordinary telephone calls concerning Government matters are permitted, subject to the usual restrictions on content. It is therefore reasonable to see whether a suitable form of access control can be devised which would allow authorised computerised access, over the PSTN, to Government data that conformed to the same restrictions. This would allow Government institutions to take full advantage of the progress in these aspects of Information Technology.

This paper discusses those possible methods of access control which are appropriate for modem connected users of computer systems which carry only UNCLASSIFIED data. The needs of secure computing are not dealt with here.

This study was initiated with the goal of developing a system for use at RSRE which would allow appropriate off-site access to those computers linked to the RSRE Data Network. This is a distributed communications system provided by the Network Services section of the Central Information Services

Division. However the issues raised during the study are, in general, applicable to other organisations.

First, as an aid to understanding the problems involved, the operation of the present land-line PSTN is considered. Then the implications of the rapidly increasing use of the cellular radio telephone links are examined, and an outline given of the operation of modems. Next the current access control methods used on central computer systems are considered along with the ways hackers exploit the weaknesses of all these links in the data transfer chain. Finally, possible solutions to the problem are suggested as the basis for an experimental investigation at RSRE. These are reported elsewhere [1].

2 Public Switched Telephone Network

How easy is it to intercept and impersonate calls on the British Telecom (BT) or Mercury telephone systems? Most of the telephone links provided by these companies are over land-lines. Some are via microwave links and, more recently, some use optical fibres. An intercept on the physical links would involve gaining access to the companies' equipment in order to attach wire taps. Usually this would be conspicuous. The micro-wave links would require quite a sophisticated receiving system to decode the traffic because of the complexity of the coding systems used to convey the data: pulse amplitude modulation; pulse code modulation etc. Also the very directional nature of the links limits the localities where such eavesdropping equipment would work.

One may conclude that the interception of ordinary telephone traffic is non-trivial and liable to be noticed; it is unlikely that most hackers would resort to such methods unless they worked for the telephone companies or had contacts within them. Of course, what is non-trivial for a school-boy may be comparatively easy for an appropriately equipped and staffed commercial organisation.

However the actual operation of the BT system, at the ordinary telephone user's level, has weaknesses which can be easily exploited using simple equipment. They allow hackers to impersonate the BT control signals to an unwary user and thereby "capture" calls. The most pertinent point about the operation of the PSTN is that, nationally, British Telecom operates a "caller release" mechanism for terminating calls.

The operation of "caller release" is best explained by an example. Let us assume that subscriber A calls subscriber B. The connection is made, they converse and then they both replace their receivers at the end of their conversation. Both would be able to make new calls virtually straight away. However, if at the end of their conversation subscriber A

(the caller) does not replace his receiver but B does, then B, on lifting his receiver again, finds that he is still connected to A; they could continue their conversation if they wished. There is no way that B can clear his line in order to make another call until A releases the line by putting his receiver down.

It follows that anybody dialling into a modem which answers the call can prevent that modem from having a clear line to dial out merely by not replacing his receiver, thus causing a denial of service.

Whilst the above is true for all public exchanges it is not necessarily so for private exchanges attached to the public network. These multi-line exchanges often implement "first party" release. In this scheme if A calls B via a private exchange and B puts his receiver down but A does not then B, upon lifting his receiver to make a call, finds that he has a clear line. The exchange has routed his outward call onto a different PSTN line. Even if the exchange has only one incoming line the action of B replacing his receiver still breaks the direct connection with A. This time A cannot hold onto B's internal exchange line. Clearly a first party release exchange would give a desirable layer of protection in any access control system.

BT have advised that it is possible to provide ordinary public telephone lines which are incoming only or outgoing only by making appropriate changes at the local exchange. Configuring lines in this manner would provide a solution to the caller release problem for those access control systems that use different telephone lines for incoming and outgoing calls. Such a course of action is obviously not applicable to access control systems that only use a single telephone line. However, as discussed below, there are other problems to be addressed as well; so other safeguards still need to be taken.

3 Evesdropping and radio links in the communications chain

Conversations over the public telephone system are not secure because of the possibilities of crossed lines as well as telephone taps. The probabilities of these occurrences in practice are small and even then the only information passed should be of little value if security directives have been followed correctly.

If however the information overheard was not that between two people but was instead the logon sequence to a computer system then the damage could be greater in that a username and password have been disclosed. At present most usernames and passwords are static, ie they do not change over long periods of time, typically many months, until explicitly

altered by the user. Under these circumstances the eavesdropper would be able to gain repeated access to that particular computer system should he know the telephone number of its remote access facility. The problem would be compounded if the legitimate user had logged-on to a further system, a not uncommon occurrence, during the time he was being overheard as now two systems would be compromised.

The advent of the cellular radio telephone service and the domestic use of cordless telephones, coupled with the rapidly expanding use of micro-computers for electronic mail display, have greatly increased the possibilities for eavesdropping. Imagine the situation where, faced with a tight schedule, somebody wishes to read his electronic mail whilst travelling in a car between meetings. This may be done by a small laptop computer and modem connected to a cellular radio telephone, a quite plausible situation. However in logging on to the electronic mail system, whether directly or by call back the user has broadcast his username and password (as well as ALL the messages) to anybody who cares to listen. Similarly the use of a cordless telephone, perhaps as a means of accessing the BT system without having to be close to a wall mounted telephone socket, carries the same eavesdropping risks.

The risk exists because these radio systems do not employ any form of scrambling. ANYBODY with a simple FM radio receiver can tune in and listen. Appropriate receivers can be bought from many electronic hobby outlets.

A prohibition on the sale of such receivers would not be a satisfactory solution because the receivers use widely available components and could be assembled by people with little technical experience.

Perhaps the greatest risk with these radio systems comes from ignorance. Many people who avail themselves of them are not yet aware of their vulnerability to eavesdropping, even for ordinary conversations. The users may be under the (false) impression that because the systems are "approved" then privacy is being guaranteed by BT and the other cellular operators to the same level as holds for present land lines. Certainly the suppliers of the systems have not publicised the problem of eavesdropping. Moreover because of the recent nature of the phenomenon, there has not been time for such information, perhaps in the form of court cases involving the eavesdropping of telephone calls, to be brought to the public's attention.

It is to be hoped that the next generation of both cellular telephones and cordless telephones will be more secure.

4 Modems and their operation

Modems are currently the key to the remote access of computers. The primary purpose of a modem (Modulator-Demodulator) is to enable two pieces of equipment (usually a computer and a terminal) designed to communicate by a direct serial binary connection to be able to do so over communication lines of limited bandwidth which do not support D.C. signal levels. These communication lines are normally ordinary telephone circuits but can also be mobile radio links.

The signalling is achieved by converting the binary levels from the computer equipment (often to the RS232C or nearly equivalent V24/28 standard) into tones of different frequencies, a method known as frequency shift keying . There are other encoding techniques, for example phase coding.

Over time two main groupings of signalling standards have evolved: those of the CCITT, used in Europe and elsewhere, and those from Bell Telephone, used in North America, Japan and some other parts of the world.

One consequence of the adoption of these standards is that modems are readily available and inexpensive. Moreover, they can be purchased with the sure knowledge that the modems used by both large and small computer systems will respond identically. This state of affairs is good for the legitimate users, but it can also be described as a hackers delight in that he can easily purchase a low cost modem and so be in a position to mount an attack on the computer systems.

Early modems were not equipped to initiate telephone calls or answer incoming calls automatically. However, recent advances in integrated circuit design coupled with the relaxation of the rules concerning equipment that can be attached to the public telephone system, has meant that nearly all modems are now supplied with these functions as standard. Such modems are equipped with simple circuits to detect the presence of the usual telephone signalling information such as the dialling tone and the ringing tone.

Unfortunately this signalling information can be relatively easily imitated. This is because modems have to be able to cope with what can be quite significant variations in signal levels and dialling tone frequencies, depending on the particular exchange to which a subscriber may be connected and the quality of the line between the subscriber and the exchange.

5 Current methods of modem access control

Modems are used in commercial/university environments to enable remote, often 24 hour, access to computer resources. They are usually attached to large systems where their use may not be monitored in any great detail. There may be many tens or hundreds attached to any one system; so individual monitoring by operators is impractical. In these systems access control is enforced by the usual methods of username-password identifiers associated with authorised users.

A typical access sequence would be as follows: the user dials the telephone number of the modem attached to the computer; once connected the computer system prompts the user for his username and password; if these are valid then the user is immediately allowed to use the computer resources. It should be noted that some access control procedures are capable of limiting remote access "privilege" to specific authorised users for their use only between specific times.

In a sense the computer access control routine has little other information to do otherwise; it does not know and cannot know the telephone number of the caller because of the dial-in nature of the access. It can neither tell whether the call is from a "legitimate" place nor give any information on locations if any hacking activity is detected. It should be noted that this state of affairs is likely to change in the long term as a consequence of the gradual change over to digital System "X" telephone exchanges and digital links to subscribers.

Some systems may make no distinction between users who are using locally connected terminals and those using remote terminals. Clearly then the use of modems merely allows hackers to get the same access as if they had physical access to local terminals. It is apparent that such systems are only as well protected as their normal procedures allow: once a hacker has the telephone number of the modem and a valid username-password then he can do as much as the legitimate user is allowed to do.

The problem of authenticating users is not new. What has changed is that hackers no longer require physical access to local, directly-connected terminals: hence systems are open to attack from many more people, who are no longer physically observable.

One answer to this problem that has been adopted by some computer systems is as follows: remote access to the system is restricted by only allowing a user to contact it from a pre-designated telephone number unique to the user. This is implemented in the following way. A user would still dial

into the system on the modem's telephone number and be asked for a username and password. If these are valid the computer system responds by telling the user to hang up and then calling the user back on the user's pre-determined number. This may be the user's home number or branch office number, whatever has been pre-agreed. The user answers the call and is asked again for identification and then, if correct, he is allowed to use the system. This approach has the advantage that even if a hacker knows a valid username-password he is only able to get the system to call the legitimate user back, thereby alerting the user to the hacker's intrusion.

Unfortunately this control policy is susceptible to a combination of modem weakness and system design. Some access control systems which employ this approach may use the SAME modem that accepted the incoming logon call to make the outgoing call. The use of caller release means that all a hacker has to do is to make the initial call, give the appropriate identifiers and then NOT break the link when requested by the computer. If now the hacker sends a dialling tone down the line the computer's modem will almost certainly assume that the line is clear and proceed to initiate the dialling. Of course the dialling sequence is not noted at the exchange. When it finishes, the hacker merely provides a ringing tone followed by the answer tone and the computer modem will think that it has been connected to the legitimate user. Of course it is actually still talking to the hacker. At this point the operating system of the computer may, on the strength of the logon validation step on dial-in, give the hacker full access to its resources with no further checks.

A partial solution to this line capture problem is to make the call back to the user on a different modem connected to a different telephone line, an approach used by the MOTOROLA Response system and others. As is discussed later, even this is not foolproof. If a hacker can discover the outgoing telephone number he can arrange to dial into this modem just as it is about to dial out and fool it in the same way.

6 Possible courses of action

A) The modem access control system must ask for user-password identification both on dial-in and dial-back

Initial thoughts have concerned the feasibility of creating a hacker resistant access control system covering external telephone access to those site computer facilities connected to RSRE's data network.

The methods proposed are based upon the idea of limiting the location of people wishing to access these systems by means of pre-arranged telephone numbers. (Note: We cannot

guarantee this completely; some users may take advantage of the ability of the cellular systems and some PABXs, to re-route calls automatically, as a way of gaining location flexibility on a single dial-back number system with all the risks of being overheard.)

Briefly the system would operate as follows: A prospective user would call a specific site number. The access control system would then ask for a username and password. If these were valid then the control system would tell the user to break the call and await a call back on the telephone number prearranged for him (his home number say). The user would only be able to gain access to computer resources after the access control system had rung him back to the prearranged telephone number and AFTER further validation.

Now weaknesses have been identified in this separate line dial-back approach caused by the operation of the public telephone network. In particular it is possible to dial into the modem that is dialling out and, providing the timing is correct, fool the outward dialling modem into believing that it has made a valid call to a legitimate user. This means that a potential hacker could call repeatedly into the outward modem until he makes a hit within the time window and gains full access to whatever computer resource the legitimate caller (who made the inward call resulting in the dial out attempt) is allowed to use. A possible solution to this problem is to attach the modem to a private exchange which implements first party release. This means that we have to rely upon the correct operation of this exchange for our protection.

Since such protection may not be guaranteed, it is proposed to add extra protection by requiring further username-password identification when the call back connection is made. If this second password proves to be invalid (perhaps after two tries) then no connection should be allowed: also the use of that username can be suspended until the user can be asked in person whether he was actually making the call. This would provide warning of potential hacker activity. Of course the reason could be innocuous, a spike of interference on the telephone line, but at least it would be investigated.

Dynamic passwords can be used to enhance protection. A dynamic password is one that is different for each access attempt. Often they are algorithmic: the computer presents the caller with a number on initial contact and the caller has to respond with another number that is derived from the computer's number by a pre-arranged secret algorithm. For example if the algorithm was to multiply the initial number by four and add one then the correct reply to the computer's prompt of 3 is 13. The other mechanism for dynamic password implementation consists of a prearranged list of passwords. The entries on this list are used in strict sequence, once

and once only, for each access attempt - this is the, so-called, one time pad method.

B) The use of data encipherment

The possible counter-measures discussed so far have assumed that the hackers could NOT overhear any communications traffic to and from these computers. All the hackers were considered able to do was to call into modem ports on computer systems, possibly exploiting weaknesses in the operation of the landline telephone service. Hence the precautions have concentrated on access control mechanisms.

However if a hacker CAN overhear a logon sequence then, provided he knows the appropriate telephone number, he may be able to gain access in a manner that would appear legitimate. Obviously a dynamic password would stop the casual listener from gaining access by mere imitation. Should the legitimate user, whose traffic is being overheard, use the initial computer as a stepping stone to further computer systems via networks such as ethernets or the various commercial/private networks, then more usernames and passwords would be revealed. So more systems would be compromised. This could threaten other systems on these networks whose operating systems do not provide all the necessary user isolation.

One solution to these problems is to encipher the traffic between the user and the computer systems. Scrambling techniques require special equipment as well as procedures for key management and distribution. One can argue that the cost in both money, and time administering such methods are such that they should only be used for information that merits it. If it were used then it would be reasonable to employ only that level of encipherment which would beyond the means of amateurs to break, so keeping costs down and simplifying key handling procedures. Such an enciphering system should have the following properties:

- i) It should comprise an add on unit, inserted between the modem port of the computer and the modem. The plain text output of the user's micro would be enciphered and passed onto the modem. The enciphered traffic from the host computer would be deciphered and passed onto the user's micro.
- ii) The interfaces would be to V24/V28 (ie RS232) standard for ease and flexibility of use.
- iii) The unit should be able to handle full duplex traffic at a speed of 9600 bps, so allowing not only for the split baud rate modems (ie 9600 into the modem but 300, say, down the telephone line) but also for the new range of 9610 bps throughput modems.

- iv) The unit should not pack the data into blocks, since this could lead to buffering problems. It could also be unnecessarily time consuming considering the short nature of many commands issued as part of a typical interactive session with computers.
- v) If possible the unit should derive its power from the modem, since most modems provide a limited supply, merely for flexibility.
- vi) The unit should be sealed, perhaps in epoxy resin, so as to reduce the chances of successful tampering.
- vii) The host computer could implement the algorithms in software so as to avoid having too many hardware units in one place.
- viii) Each unit would have a different in-built password uniquely related to the individual username.
- ix) The unit would be provided with a method of switching between clear (no enciphering) operation and ciphered operation.

A possible log on sequence would be as follows:

First the user would ensure that the unit is set to clear. The user would then dial the desired system and be asked for a username. This he would provide. Next he is asked for the password, but before it is sent he changes over to ciphered operation. If the computer system accepts the password then it calls the user back on the prearranged telephone number. The system then asks again for a username and password but this time they are different and enciphered. If they are valid then the session proceeds all in enciphered mode.

The initial contact has to be in clear so as to allow the computer to select the appropriate deciphering key. It also gives the user a chance to recover from any setup errors he may have made in the choice of baud rate, parity etc.

7 Are ALL the techniques ALWAYS applicable ?

A range of techniques have been discussed that would reduce the vulnerability of computers to hacking : separate dial-back lines, dynamic passwords and encipherment. Each technique has its different strengths and weaknesses as well as capital and administrative costs. We have seen that the use of all of them in a system will give the greatest protection. However, other considerations may outweigh the use of some of them.

For example a system manager may not want either to bear the cost of dial-back calls or to apportion them for operational reasons. He might wish to have a system that was dial-in only.

Other system managers may consider that, for the information stored on their systems, the problems of key management for encrypted links outweigh the privacy benefits.

In the end the final judgment as to the appropriate mix of techniques rests with the system manager based upon his knowledge of the particular data stored on the system and the access style needed for the users of the system.

8 Conclusions

It has been shown that it is possible to devise access control methods which provide protection against the class of hacker who can exploit the weaknesses of the present telephone system. These methods use the techniques of (i) separate dial-back lines (ii) dynamic passwords and (iii) encipherment; even so, they will not give complete protection. Furthermore the proliferation of usernames and passwords, static or dynamic, raises the problem that the legitimate user may find that he has too much to remember and so try to simplify the choices, thereby weakening the protection.

A potential problem has been identified arising from eavesdropping if remote access is attempted over links which involve the use of cordless telephones or the new cellular radio telephone system. This problem is likely to get worse because of rapid growth in the use of such systems. It will be exacerbated if users deliberately use the cellular systems in preference to land-line systems purely for their ability to re-route calls automatically.

One short term solution to the radio link problem would be to prohibit its use for remote access purposes. More generally, however we consider that some form of encryption is desirable in order to provide protection against radio links being unknowingly used. Furthermore such a solution would also defeat most of the existing land line hacker problems.

Reference

- [1] Giess S.C., "Experiments into the control of access to computer resources via the Public Telephone System", RSRE Memorandum No. 4155

DOCUMENT CONTROL SHEET

UNCLASSIFIED

Overall security classification of sheet

(As far as possible this sheet should contain only unclassified information. If it is necessary to enter classified information, the box concerned must be marked to indicate the classification eg (R) (C) or (S))

1. DRIC Reference (if known)	2. Originator's Reference	3. Agency Reference	4. Report Security U/C	Classification
	REPORT 88006			
5. Originator's Code (if known) 778400	6. Originator (Corporate Author) Name and Location Royal Signals and Radar Establishment St Andrews Road, Malvern, Worcs. WR14 3PS			
5a. Sponsoring Agency's Code (if known)	6a. Sponsoring Agency (Contract Authority) Name and Location			
7. Title ON THE PRIVACY PROBLEMS INVOLVED IN ALLOWING ACCESS TO COMPUTERS VIA THE PUBLIC TELEPHONE SYSTEM				
7a. Title in Foreign Language (in the case of translations)				
7b. Presented at (for conference papers) Title, place and date of conference				
8. Author 1 Surname, initials Giess, S.C.	9(a) Author 2	9(b) Authors 3,4...	10. Date 1988.04	cc. ref. 11
11. Contract Number	12. Period	13. Project	14. Other Reference	
15. Distribution statement				
Descriptors (or keywords)				
continue on separate piece of paper				
Abstract This report discusses some privacy problems involved in allowing access to computers over the Public Switched Telephone Network (PSTN). The relevant aspects of current land-line PSTN and cellular radio operations are described and the weaknesses of the access controls of current computer systems are discussed. Possible solutions that would allow access under a limited set of conditions are described.				